HOW DO I KNOW IF A MAIL IS AUTHENTIC?

Through the email of the University of Valencia, we coordinate and solve a multitude of work and academic tasks in our day to day.

Sometimes, the rush and routines do not apply all the security measures that would be necessary when using this tool, something that cybercriminals use to carry out their deception purposes.

One of the most common cases is what we know as email spoofing or phishing by email. Through this malicious technique emails are sent with a false sender to send spam, spread malware or carry out phishing attacks and supplant the identity of company executives, suppliers, customers, etc.

The increasingly refined methods of cybercriminals make it difficult to distinguish legitimate mail from one that is not. But, do not worry, we will give you an advantage by explaining the necessary guidelines for you to identify when you are receiving these types of messages.

Interpreting the email headers you will be able to identify, among others, the following data:

- The information related to the sender and the receiver,
- the intermediate mail servers through which mail passes from the origin to its destination,
- the mail client that was used to send it, and
- the date of sending and receiving the email.

All this information is in the headers or headers of the emails.

A part that with the naked eye is hidden, we can visualize it with a couple of clicks.

How do I access email headers?

Mail clients for Windows

Classic Interface:

- In the email we want to analyze we will see a tab on the right side, click on it.

- We will show the header of the email with a lot of information that we will see later how to analyze it through the help of a program.

Advanced interface (postman):

- In this email interface, simply by right clicking on the email, a menu will appear, to which we will select the option “See original message format”
• We will show the header of the email with a lot of information, which we will later copy and follow the instructions in **STEP 1** detailed below.

**STEP 1**

• Google has a tool to analyze email headers, which can be entered in 'plain text', to give us information of some relevance about email.

https://toolbox.googleapps.com/apps/messageheader/?lang=en

When clicking on **ANALYZE HEADER**, you must pay attention to the SFP parameter:

- There will tell you when it is a ‘clean’ email SFP: pass
- When it is a malicious or suspicious email, it will provide you with information of interest for decision making.

It must be said that Google has very immediate and exhaustive measures of filtering for emails that are received on its servers, so the analysis is quite effective and reliable.

**Microsoft Outlook 2016, 2013 and 2010**

1. Double-click the suspicious email to open it outside the reading pane.
2. Select the option **File> Properties**.

![Image of Microsoft Outlook properties](image)

1. The header information is displayed in a new window, in the "Internet headers" section, such as the one shown in the image.
Mozilla Thunderbird

1. Open the email you want to analyze.
2. Click on the “More” > “See source code” buttons, located in the upper right part of the window.

Mail headers will be displayed in a new window.

Mail clients for Mac

Mail for Mac

1. Access the email you want to see the headers.
2. Go to “Display” > “Message” > “All headers.”
1. Next, the full email header will be displayed.

Web mail clients

Gmail

1. Open the email whose headers you want to get.
2. Then, click on the dotted line to the right of the "Reply" icon.
3. Click on "Show original".

1. The full email header will be displayed in a new tab.

Outlook

1. Open the email you want to analyze.
2. Then click on the dotted line to the right of the "Resend" option
3. Click on "See message origin".
1. The headers will be displayed in a new window.

Yahoo

1. Select the email whose headers you want to view.
2. Then click on the dotted line icon “View plain message”.

1. The full email header will be displayed in a new window.

How are headers interpreted?

Now that we know how to obtain the headers, we will explain their content to know if we are facing a fraudulent email.

Example of legitimate mail:
First, we note that the mail was delivered in 1 second ("Delivered after 1 sec") which means that it took 1 second to reach its recipient since it was sent (in the last highlight you can see the addresses of the servers by which passes the mail until it is delivered). As will be seen in the following example, excessive delivery time is usually indicative of fraudulent mail.

In the "From:" field we see that the domain linkedin.com matches the sender of the message we received (no impersonation).

The registers SPF, DKIM Y DMARC They have been verified correctly. Although it is quite intuitive to interpret the verification of these records through this tool, you can check more information about the SPF, DKIM and DMARC records in Header of spam messages.

**Example of illegitimate mail:**

The mail was delivered after 2 hours, that is, it took 2 hours to arrive from when it was sent (in the last highlight you can see the addresses of the servers through which the mail passes until it is delivered).

In the "From:" field we observe that the chukzem.xyz domain does not match the supposed issuer of the message that in this case claims to be a sales company online.

DKIM and DMARC records have not passed verification control. Both the delivery time, as the sender and the SPF, DKIM and DMARC records are indicating that it is a clear example of email spoofing.

Now you have no excuses, you know how to avoid falling into the trap of cybercriminals. Be careful with your email and protect your work, and that of your classmates at the University of Valencia.